UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/726,822	11/29/2000	Olivier Guiter	PALM-3535.US.P	2236

7590 02/17/2005

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/726,822	**Applicant(s)** GUITER ET AL.	
	Examiner Shin-Hon Chen	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4 and 6-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4 and 6-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3, 4, 6-26 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, 4, 6, 8-13, and 17-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clark in view of Varadharajan et al. U.S. Pat. No. 5887063 (hereinafter Vara) and further in view of Kikinis et al. U.S. Pat. No. 5600800 (hereinafter Kikinis).

4. As per claims 1, Clark discloses a method for preventing unauthorized transfer of data between a portable computer system and systems of data storage and communication including an other computer (Clark: [0009]-[0011]), said method comprising the steps of:

a) automatically receiving identification authentication information for said portable computer system, wherein said authentication information comprises a unique identity for said portable computer (Clark: [0060]);

b) comparing said identification authentication information with a list of authorized portable computer system identities (Clark: [0060]);

c) determining whether said portable computer system identity is authorized based on said identification authentication information and said unique identity (Clark: [0060]);

d) enabling communication between said portable computer system and said other computer provided said identity is authorized and disabling said communication if said identity is not authorized (Clark: [0060]);

Clark does not explicitly disclose e.) enabling decryption of encrypted data from said portable computer system provided said identity is authorized and disabling decryption if said identity is not authorized. However, Vara discloses enabling the portable computer to communicate with host by establishing secure key for secure communication after authentication has been completed (Vara: column 4 line 54 – column 5 line 31). It would have been obvious to one having ordinary skill in the art to enable/disable encryption based on authentication because it is well known in the art to have secure communication between two devices. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Vara within the system of Clark because it increases system security by communicating encrypted data/information after authentication has been completed to provide additional security.

Clark as modified further discloses wherein step a) comprises the step of transferring identification authentication information between a portable computer system portable device and a communication interface device (Clark: figures 1a-c and [0009]-[0011] and [0060]) and said portable device is a palmtop computer and said interface device is a palmtop computer system cradle (Clark: [0009]-[0011]).. Clark as modified does not explicitly disclose transferring authentication from communication interface device to portable computer. However, Kikinis discloses that limitation (Kikinis: column 10 line 50 – column 11 line 24). It would have been obvious to allow bi-directional authentication to authenticate the device that seeks to retrieve information from the other device. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Kikinis within the combination of Clark-Vara because it's well known in the art to authenticate requesting device prior to access.

5. As per claim 3, Clark as modified discloses the method as recited in Claim 2. Clark as modified further discloses wherein said information is transferred from said portable device to said interface device to uniquely identify said portable device to said interface device (Clark: [0060]).

6. As per claim 4, Clark as modified discloses the method as recited in Claim 2. Clark as modified further discloses wherein said information is transferred from said interface device to said portable device to uniquely identify said interface device to said portable device (Kikinis: column 10 lines 50 – column 11 line 24).

7. As per claim 6, Clark as modified discloses the method as recited in Claim 1. Clark as modified further discloses wherein said step b) comprises the steps of: recognizing said identification authentication information as an indication of unique identity of the source sending said information (Clark: [0060]) and indexing said unique identity to a list of programmed identities (Clark: [0060]). Kikinis also discloses these limitations (Kikinis: column 11 lines 8-15). Same rationale applies here as above in rejecting claim 2.

8. As per claim 8, Clark as modified discloses the method as recited in Claim 1. Clark as modified further discloses wherein said step d) comprises the steps of allowing said portable

computer to synchronize with said other computer upon authorization of communication and preventing synchronization upon prohibition of communication (Clark: [0060]).

9. As per claim 9, Clark as modified discloses the method as recited in Claim 1. Clark as modified further discloses wherein step e) comprises the steps of disclosing a specific key value with which said data is encrypted upon authorization of communication and not disclosing said specific key value upon prohibition of communication (Vara: column 4 line 54 – column 5 line 31).

10. As per claim 10, Clark discloses a system for preventing unauthorized transfer of data between a portable computer system and a host system (Clark: [0009]-[0011] and [0060]), comprising:

a) a portable computer device capable of synchronizing with said host (Clark: figures 1a-c and [0009]-[0011]);

b) an interface device compatible to receive said portable computer device and coupled with said host system and capable of facilitating communication between said portable computer device and said host system (Clark: figures 1a-c and [0009]-[0011]);

c) an identification authenticating component incorporated into one of said devices and providing a unique identification signal corresponding to the unique identity thereof (Clark: [0009]-[0011] and [0060]); and d.) an identification authorizing component capable of determining if said unique identity is authorized for synchronization and for correspondingly enabling and disabling synchronization between said portable computer and said host system (Clark: [0060]).

Clark does not explicitly disclose e.) enabling decryption of encrypted data from said portable computer system provided said identity is authorized and disabling decryption if said identity is not authorized. However, Vara discloses enabling the portable computer to communicate with host by establishing secure key for secure communication after authentication has been completed (Vara: column 4 line 54 – column 5 line 31). It would have been obvious to one having ordinary skill in the art to enable/disable encryption based on authentication because it is well known in the art to have secure communication between two devices. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Vara within the system of Clark because it increases system security by communicating encrypted data/information after authentication has been completed to provide additional security.

11. As per claim 11 and 12, Clark discloses a system as in Claim 10. Clark further discloses wherein said portable computer device is a palmtop computer and said interface device is a palmtop computer cradle (Clark: [0009]-[0011]).

12. As per claim 13, Clark discloses a system as in Claim 10. Clark does not explicitly disclose wherein said synchronous communication is further encrypted with a specific key value from said identification authenticating tagging component such that unauthorized applications external to said portable computer system are locked out from deciphering data therefrom.

However, Vara discloses that limitation (Vara: column 4 line 54 – column 5 line 31). It would have been obvious to one having ordinary skill in the art to combine the teachings of Vara within the system of Clark because it increases system security by communicating encrypted data/information after authentication has been completed to provide additional security.

13. As per claim 17. Clark discloses a system as in Claim 10. Clark further discloses wherein said identification authorizing component is a software program (Clark: [0060]). Computers require the combination of software and hardware to accomplish authentication tasks.

14. As per claim 18, Clark discloses a system as in Claim 10. Clark further discloses wherein said identification authenticating tagging component is in direct electrical connection with said identification authentication reading component via contacts (Clark: [0009]-[0011] and figures 1a-c).

15. As per claim 19, Clark discloses a system as in Claim 10. Clark does not explicitly disclose wherein said identification authenticating tagging component is in contact free communication with said identification authentication reading component via an infrared communication mechanism. However, Vara discloses that limitation (Vara: column 4 lines 22-34). It would have been obvious to one having ordinary skill in the art to combine the teachings of Vara within the system of Clark because it is well known in the art to use various types of product for transmitting signals between two devices.

16. As per claim 20, Clark as modified discloses a system as in Claim 9. Clark as modified further discloses wherein said identification authenticating tagging component is in contact free communication with said identification authentication reading component via a transmitter/receiver modality and antenna array (Vara: column 4 lines 22-34).

17. As per claim 21, Clark discloses a system for preventing unauthorized transfer of data between a portable computer system and a system of data storage and communication, comprising:

a) a portable computer device capable of synchronizing with said system of data storage and communication (Clark: [0009]-[0011] and figures 1a-c);

b) an interface device compatible to receive said portable computer device and coupled with said system of data storage and communication and capable of facilitating communication between said portable computer device and said system of data storage and communication (Clark: [0009]-[0011] and figures 1a-c);

d.) an identification authentication reading component capable of sensing and reading said unique identification signal incorporated into the other of said devices not incorporating said tagging component (Clark: [0060]);

e.) an identification authorizing component receiving input from said reading component and incorporated into the same one of said devices as said reading component, capable of determining if said unique identity is authorized for synchronization and of correspondingly enabling and disabling synchronization between said portable computer and said system of data storage and communication (Clark: [0060]).

Clark does not explicitly disclose c) an identification authenticating tagging and data encryption keying component incorporated into one of said devices and providing a unique identification signal and an encryption key cipher value corresponding to the unique identity thereof; and f.) an identification authorizing component further capable of enabling deciphering of encrypted communication from said portable computer device if said unique identity is authorized and disabling decryption if said unique, identity is unauthorized.

However, Vara discloses the portable device returns data for authentication regarding keys (Vara: column 5 lines 32 – 55) and authenticate if the received value is valid and establish secure key for communication if authentication is successful (Vara: column 4 line 54 – column 5 line 31). It would have been obvious to combine the teachings of Vara within the system of Clark because it increases security by authenticate using key algorithms in addition to identification authentication.

Clark as modified discloses a host computer authenticates portable computer but not vice versa. However, Kikinis discloses a portable computer authenticates a host computer when the host computer tries to access data stored within the portable computer (Kikinis: column 10 line 50 – column 11 line 24). It would have been obvious to allow bi-directional authentication to authenticate the device that seeks to retrieve information from the other device. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Kikinis within the combination of Clark-Vara because it is well known in the art to authenticate requesting device prior to access.

18. As per claim 22, Clark as modified discloses a system as in Claim 20. Clark as modified further discloses wherein said identification authorizing component incorporates software for determining if said unique identity is authorized for synchronization, for correspondingly enabling and disabling synchronization, and deciphering encrypted data from said portable computer device (Vara: column 4 lines 54 – column 5 line 31).

19. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clark in view of Vara and further in view of Kikinis and further in view of Frederick U.S. Pat. No. 6157825 (hereinafter Frederick).

20. As per claim 7, Clark as modified discloses the method as recited in Claim 1. Clark as modified further discloses wherein said step c) comprises the steps of: reacting to positive indexing match as an authenticated authorized identity (Clark: [0060]); and authorizing communications enablement in response to an authenticated authorized identity, and prohibiting communications in response to an unauthorized identity (Clark: [0060]). Clark does not explicitly disclose reacting to negative indexing match as an unauthorized identity. However, Frederick discloses checking both authorized list and unauthorized list for authentication (Frederick: column 5 line 60 – column 6 line 35). It is well known in the art to check authorized users and unauthorized users. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Frederick within the combination of Clark-Vara because checking authorized and unauthorized offers other options for users who are neither authorized nor unauthorized users.

21. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clark in view of Pickholtz U.S. Pat. No. 4593353 (hereinafter Pickholtz).

22. As per claim 14, Clark discloses a system as in Claim 10. Clark does not explicitly disclose wherein said identification authenticating tagging component is a magnetic key and said identification authentication reading component is a magnetic key reader. However, Pickholtz discloses using magnetic key to achieve identification and authentication (Pickholtz: column 1 lines 39-45). It would have been obvious to one having ordinary skill in the art to combine the teachings of Pickholtz within the system of Clark because identification authentication can apply to various types of products including magnetic keys.

23. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clark in view of Graves U.S. Pat. No. 5239166 (hereinafter Graves).

24. As per claim 15, Clark discloses a system as in Claim 10. Clark does not explicitly disclose wherein said identification authenticating tagging component is a smart card and said identification authentication reading component is a smart card reader. However Graves discloses that limitation (Graves: column 2 line 29 – column 3 line 32). It would have been obvious to one having ordinary skill in the art to combine the teachings of Graves within the system of Clark because identification authentication can apply to various types of products including smart card, which is well known in the art.

25. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clark in view of Kelly et al. U.S. Pat. No. 6480101 (hereinafter Kelly).

26. As per claim 16, Kelly discloses a system as in Claim 10. Kelly does not explicitly disclose wherein said identification authorizing component is an application specific integrated circuit. However, Kelly discloses that limitation (Kelly: abstract and column 2 line 30-55 and column 3 lines 32-57). It is well known in the art that ASIC is very difficult to tamper with and good for conducting authentication purposes. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Kelly within the system of Clark.

27. Claims 23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clark in view of Kikinis.

28. As per claim 23, Clark discloses a communication system comprising: a host computer system comprising a communication port (Clark: figures 1a-c and [0009]-[0011]); a portable electronic device comprising a communication port and an identity reference (Clark: figures 1a-c and [0009]-[0011] and [0060]); and a communication module for coupling between said communication ports of said portable electronic device and said host computer system (Clark: figures 1a-c and [0009]-[0011] and [0060]), and disallowing communication between said portable electronic device and said host computer system if authentication failed (Clark: [0060]).

Clark does not explicitly disclose said communication interface module comprising: an authentication device for authenticating said identity reference; and a communication interface circuit coupled to said authentication device and for allowing communication between said portable electronic device and said host computer system provided said authentication device indicates a proper authentication of said identity reference. However, Kikinis discloses these limitations (Kikinis: figure 41 and column 10 line 50 – column 11 line 15). It would have been obvious to one having ordinary skill in the art to combine the teachings of Kikinis within the system of Clark because it reduces data transmission between devices.

29. As per claim 25, Clark as modified discloses a communication system as described in Claim 23. Clark as modified further discloses wherein said communication module contains a slot for receiving said communication port of said electronic device (Kikinis: figures 5, 6, and 41).

30. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clark in view of Kikinis and further in view of Vara.

31. As per claim 24, Clark as modified discloses a communication system as described in Claim 23. Clark as modified does not explicitly disclose wherein said communication interface circuit comprises a decryption circuit. However, Vara discloses that limitation (Vara: column 4 lines 35-43 and figure 1). It would have been obvious to include the decryption circuit in the communication interface, which is coupled to the host computer to decrypt encrypted data

communication from the host computer and portable computer. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Vara within the combination of Clark-Kikinis because allow secure communication between the portable computer and host computer.

32. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Clark in view of Kikinis and further in view of Kramer U.S. Pat. No. 6286099 (hereinafter Kramer).

33. As per claim 26, Clark as modified discloses a communication system as described in Claim 23. Clark as modified does not explicitly disclose wherein said identity reference is stored on a removable smart card. However, Kramer discloses that limitation (Kramer: column 4 lines 18-25). It is well known in the art to use smart card to enable devices to receive data/services. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Kramer within the combination of Clark-Kikinis.

Response to Arguments

34. Applicant's arguments filed on 8/25/04 have been fully considered but they are not persuasive.

35. According to applicant's argument on the Clark reference, applicant argues that Clark does not disclose enabling decryption of encrypted data from the handheld computer provided the identity of the handheld computer is authorized and disabling decryption if the identity is not authorized. However, Clark reference is not relied upon for that limitation. Instead, Vara

reference is used to disclose that limitation (Vara: column 4 line 62 – column 5 line 31). Also, Clark discloses using unique serial number to authenticate handheld device prior to communication (Clark: [0060]). Therefore, the argument is respectfully traversed.

36. According to applicant's argument on the Vara reference, applicant argues that Vara reference does not disclose the portable device is docked with a cradle or support means. However, Vara reference is applied to indicate method of allowing encrypted communication between two devices when authentication is successful and it would have been obvious to one having ordinary skill in the art to apply this method to enable secure communication between devices. Therefore, applicant's argument is respectfully traversed.

37. According to applicant's argument on Kikinis reference, applicant argues that the Kikinis reference does not disclose automatically transfer identity information. However, Clark reference discloses automatically comparing the unique identification when the portable device is detected (Clark: [0060]) and Kikinis reference also discloses comparing embedded ID code (Kikinis: column 11 lines 8-15). Kikinis reference discloses querying password when there is no matching ID codes. Therefore, applicant's argument is respectfully traversed.

38. According to applicant's argument on Frederick reference, applicant argues that Frederick reference relates to wireless subscriber systems. However, Frederick reference is applied to indicate a method of authentication by comparing both authorized and unauthorized list before communication can be initiated. Therefore, it would have been obvious to one having ordinary skill in the art to apply this authentication method to allow secure communication between two devices.

39. According to applicant's argument on Pickholtz, Kelly, and Kramer, applicant argues the method disclosed by Pickholtz, Kelly, and Kramer respectively. However, the references are merely used to indicate that product that are well known in the art to provide identification authentication. Therefore, the arguments do not relate to what was applied in the office action.

40. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

41. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC
S.C.

Gregg J. Lamarre
Primary Examiner